

ABSTRACT

A system and method that provides for copying ARP replies, and generating data packets which include the ARP reply, and other information such as an identification of the port on the ARP reply was received. These data packets are then transmitted to an ARP collector which stores the ARP reply and port information. The ARP collector then uses this stored information, and analyzes future data packets relative to the stored information to detect occurrences of ARP spoofing. The ARP collector further provides for generating alerts and taking security actions when ARP reply spoofing is detected.

10